Amendments to the Specification:

Please replace the paragraph beginning on page 3, line 1 with the following rewritten paragraph:

Both MD5 and SHA1 specify that data is to be processed in 512-bit blocks. If the data in a packet to be processed is not of a multiple of 512 bits, padding is applied to round up the data length to a multiple of 512 bits. Thus, if a data packet that is received by a chip for an authentication is larger then 512 bits, the packet is broken into 512-bits data blocks for authentication processing. If the packet is not a multiple of 512 bits, the data left over following splitting of the packet into complete 512-bit blocks must be padded in order to reach the 512-bit block processing size. The same is true if a packet contains fewer [[then]] <u>than</u> 512 bits of data. For reference, a typical Ethernet packet is up to 1,500 bytes. When such a packet gets split into 512-bit blocks, only the last block gets padded and so that overall a relatively small percentage of padding overhead is required. However for shorter packets, the padding overhead can be much higher. For example, if a packet has just over 512 bits it will need to be divided into two 512-bit blocks, the second of which is mostly padding so that padding overhead approaches 50% of the process data. The authentication of such short data packets is particularly burdensome and time consuming using the conventionally implemented MD5 and SHA1 authentication algorithms.

Please replace the paragraph beginning on page 4, line 11 with the following rewritten paragraph:

Moreover, the HMAC-MD5-96 and HMAC-SHA1-96 algorithms used in IPSec expand MD5 and SHA1, respectively, by performing two loops of operations. The HMAC algorithm for either MD5 or SHA1 (HMAC-x algorithm) is depicted in Fig. 1. The inner hash (inner loop) and the outer hash (outer loop) use different initial hash states. The outer hash is used to compute a digest based on the result of the inner hash. Since the result of the inner hash is 128 bits long for MD5 and 160 bits long for SHA1, the result must always be padded up to 512 bits and the outer hash only processes the one 512-bit block of data. HMAC-MD5-96 and HMAC-SHA1-96 provide a higher level of security, however additional time is needed to perform the outer hash operation. This additional time becomes significant when the length of the data to be processed is short, in which case, the time required to perform the outer hash operation is comparable to the time required to perform the inner hash operation.

Please replace the paragraph beginning on page 5, line 1 with the following rewritten paragraph:

Authentication represents a significant proportion of the time required to complete cryptography operations in the application of cryptography protocols incorporating both encryption/decryption and MD5 and/or SHA1 authentication functionalities. In the case of IPSec, authentication is often

the time limiting step, particularly for the processing [[or]] of short packets, and thus creates a data processing bottleneck. Accordingly, techniques to accelerate authentication and relieve this bottleneck would be desirable. Further, accelerated implementations of multi-round authentication algorithms would benefit any application of these authentication algorithms.

Please replace the paragraph beginning on page 7, line 3 with the following rewritten paragraph:

In one aspect, the present invention pertains to an authentication engine architecture for [[an]] a multi-loop, multi-round authentication algorithm. The architecture includes a first instantiation of a multi-round authentication algorithm hash round logic in an inner hash engine, and a second instantiation of a multi-round authentication algorithm hash round logic in an outer hash engine. A dual-frame payload data input buffer configured for loading one new data block while another data block [[one]] is being processed in the inner hash engine, an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations, and a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines are also included. The multi-loop, multi-round authentication algorithm may be HMAC-MD5 or HMAC-SHA1.

Please replace the paragraph beginning on page 7, line 14 with the following rewritten paragraph:

In another aspect, the invention pertains to an authentication engine architecture for a multi-round authentication algorithm. The architecture includes a hash engine configured to implement hash round logic for a multi-round authentication algorithm. The hash round logic implementation ~~included~~ <u>includes</u> at least one addition module having a plurality of carry save adders for computation of partial products, and a carry look-ahead adder for computation and propagation of a final sum. The multi-round authentication algorithm may be MD5 or SHA1.

Please replace the paragraph beginning on page 17, line 2 with the following rewritten paragraph:

As described above, both MD5 and SHA1 algorithms specify that the final hash states of every 512-bit block <u>are</u> to be added together with the initial hash states. The results are then used as the initial states of the next 512-bit block. In MD5, values of four pairs of 32-bit registers need to be added and in SHA1, five pairs. Considering that each 32-bit addition takes one clock cycle, a typical hardware implementation would use four extra cycles in MD5 and five extra cycles in SHA1 to perform these additions if hardware resources are limited.